

(19)



Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 1 089 180 A1

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:
04.04.2001 Bulletin 2001/14

(51) Int. Cl.⁷: **G06F 11/273**, G06F 11/22

(21) Application number: **00120098.9**

(22) Date of filing: **15.09.2000**

(84) Designated Contracting States:
**AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE**
Designated Extension States:
AL LT LV MK RO SI

(72) Inventors:
• Hayashi, Yasuhiro
Minato-ku, Tokyo (JP)
• Kido, Masahiro
Minato-ku, Tokyo (JP)

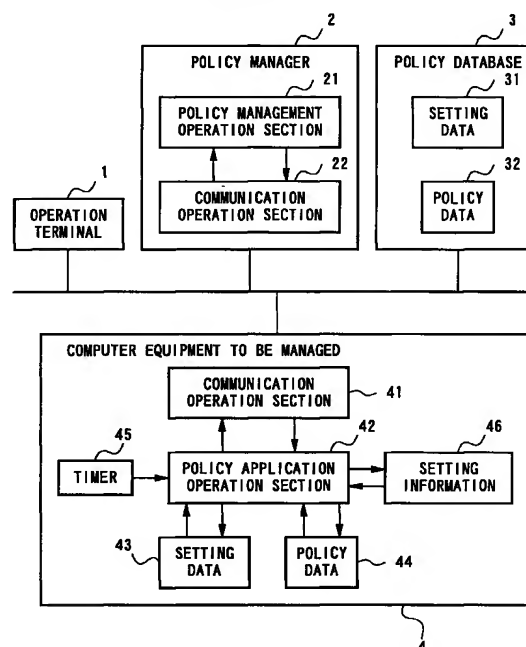
(30) Priority: **16.09.1999 JP 26257399**

(74) Representative: **Betten & Resch**
Reichenbachstrasse 19
80469 München (DE)

(71) Applicant: **NEC CORPORATION**
Tokyo (JP)

(54) **Distributed remote management method for computer equipment**

(57) A distributed remote management method for computer equipment is provided for automatically detecting a modification, when setting information is altered due to carelessness or the like, and performing restoration of the setting information or notification to an administrator according to a predetermined policy, to thereby maintain an appropriate condition. A policy management operation section (21) delivers setting data (31, 43) and policy data (32, 44) input by an administrator from an operation terminal (1) to a policy database (3) and to computer equipment to be managed (4) for storage. A policy application operation section (42) activated at regular intervals reads out the setting data (43) and the setting information (46) for comparison. As a result of this comparison, if a disagreed item is found, a corrective action held in the policy data (44) is read out with regard to the disagreed item, and a countermeasure according to a definition in the corrective action is executed. The setting information is maintained by means of such distributed processing.

FIG. 1

Description

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] The present invention relates to a distributed remote management method for computer equipment for managing and maintaining the setting information of computer equipment based on a previously defined policy.

[0002] This application is based on Japanese Patent Application No. Hei 11-262573 (Unpublished), the contents of which are incorporated herein by reference.

Description of the Related Art

[0003] Recently, the importance of computer networks in industries is increasing, and the number of computers connected to networks is also increasing. In such intra-organization computer networks, there are data showing that management expenses are overwhelmingly larger than the cost of computer equipment itself. Accordingly, there is a demand for a technique which can efficiently manage a plurality of computers connected to a network at a low cost. Moreover, in view of controlling security, it is important to maintain the consistency of settings of various equipment connected to the network, by means of a centralized control.

[0004] In such a situation, unified management of various setting information of respective computer equipment through the medium of the network, provides a large advantage in cost. As a result, tools for performing unified management have already been put to practical use and utilized. Moreover, as for the security aspect, an apparatus has been invented which manages and maintains network security by preparing a security policy in an open distributed environment, as disclosed for example, in Japanese Unexamined Patent Application, First Publication No. Hei. 7-141296.

[0005] As described above, techniques which can perform unified management of setting information of computer equipment over a whole network have been provided, and an overall administrator who generalize the whole network receive a benefit from these techniques. On the other hand, since it is also possible to set respective computer equipment individually, there may be a case where individual administrators of the computer equipment make an inappropriate setting due to carelessness, or a case where an attacker being a third party changes the setting maliciously.

[0006] That is to say, it is important that the setting information by means of unified management always coincides with the information set in the actual computer equipment. Nevertheless, with the related art, it is not possible to appropriately cope with disagreement which may arise in the above described situation.

SUMMARY OF THE INVENTION

[0007] In view of the above situation, it is an object of the present invention to provide a distributed remote management method for computer equipment in which not only setting of the computer equipment to be managed is performed, but also the above described disagreement is detected by a function provided in the computer equipment to be managed itself, to thereby automatically perform appropriate countermeasure, so that as a result, the setting information is maintained in an appropriate condition.

[0008] To solve the above problem, with the present invention, a policy management operation section or the like in a management server connected to the network, collectively holds and manages specified values (setting data) related to the setting information and the countermeasures (policy data). That is, since these specified values and countermeasures are uniformly managed on the management server side, it becomes possible for an administrator to input and edit these on an operation terminal operated by the administrator. As a result, the computer equipment to be managed connected to the network can be efficiently controlled collectively, enabling a decrease in management expenses.

[0009] Moreover, the above described specified values are held in the computer equipment to be managed, and compared with set values actually set as the setting information of the computer equipment to be managed. Then, detection of disagreement between the specified value and the set value is made. Moreover, if there is disagreement between these, a policy in the countermeasure specified in advance and held on the computer equipment to be managed is referred to, and a corresponding corrective action is automatically executed for each item in which disagreement is detected.

[0010] Accordingly, it is possible to detect a situation where the setting information on the computer equipment to be managed is altered and disagrees with the specified value, due to carelessness of an administrator of individual computer equipment to be managed, or malicious intention of an attacker being a third party. Hence, suitable action can be taken, such as automatic restoration of the setting information, notification to the administrator by means of automatic mail transmission or the like, depending on the corrective action specified in the countermeasures. As a result, it becomes possible to maintain the setting information of the whole system as per the intention of the administrator, thereby enabling protection against attacks from an attacker or the like.

[0011] In addition, the specified values, the countermeasures, and the setting information are all held in the computer equipment to be managed, and processing for applying the policy is executed on the computer equipment to be managed. Therefore in the course of this processing, the imposition of a burden on the network resources due to the flow of the data of the speci-

fied values, the countermeasures, and the setting information, can be avoided.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012]

FIG. 1 is a block diagram showing a construction for realizing a structure for setting information management according to one embodiment of the present invention.

FIG. 2 is a flow chart showing a processing of a policy management operation section according to the embodiment.

FIG. 3 is a flow chart showing a processing of a policy application operation section according to the embodiment.

FIG. 4 is a diagram showing an example of a data structure for setting data according to the embodiment.

FIG. 5 is a diagram showing an example of a data structure for policy data according to the embodiment.

DESCRIPTION OF THE PREFERRED EMBODIMENT

[0013] One embodiment of the present invention will now be described with reference to the drawings. FIG. 1 is a block diagram showing a construction of a policy manager (management server) and computer equipment to be managed according to the embodiment of the present invention. In this figure, reference symbol 1 denotes an operation terminal for performing input and editing of setting information, 2 denotes a policy manager, 3 denotes a policy database managed by the policy manager 2, and 4 denotes computer equipment to be managed.

[0014] The policy manager 2 is provided with a policy management operation section 21 and a communication operation section 22. Setting data 31 (specified values) of the computer equipment to be managed 4 and policy data 32 (countermeasures) input from the operation terminal 1 by an administrator, are notified from the policy management operation section 21 to the policy database 3. The policy database 3 holds these setting data 31 and policy data 32.

[0015] In the computer equipment to be managed 4, reference symbol 41 denotes a communication operation section, 42 denotes a policy application operation section (management unit), and 45 denotes a timer. Moreover, 43 denotes setting data (specified values), and 44 denotes policy data (countermeasures), and these setting data 43 and policy data 44 are transferred from the policy management operation section 21 via the communication operation section 22 and the communication operation section 41 to the policy application operation section 42, and written in a memory (not shown). Contents of the setting data 43 and the policy

data 44 will be described later.

[0016] Moreover, 46 denotes setting information. The setting information is set by the policy application operation section 42 based on the setting data 43, and when the computer equipment to be managed 4 actually operates, the set values written in the setting information 46 are referred to.

[0017] In FIG. 1, only one computer equipment to be managed 4 is shown, but there may be any number of computer equipment to be managed 4.

[0018] Next, the operating procedure in this embodiment will be described. FIG. 2 is a flow chart showing a procedure for setting the setting data 43 and the policy data 44.

[0019] At first, in step S101 in FIG. 2, an administrator inputs the setting data (that is, values to be set) and the policy data (that is, countermeasures when incorrect data is detected in each item), for each computer equipment to be managed and each item of setting information, through the operation terminal 1.

[0020] Next, in step S102, the policy management operation section 21 in the policy manager 2 receives the input setting data and policy data, and in step S103, records these data on the policy database 3 as the setting data 31 and the policy data 32.

[0021] Then, in step S104, the policy management operation section 21 notifies the above described setting data and policy data via the communication operation section 22 and the communication operation section 41 to the policy application operation section 42 in the computer equipment to be managed 4 to which the setting data and policy data are applied.

[0022] In step S105, the policy application operation section 42, which has received these data, writes these data to a memory provided in the computer equipment to be managed 4 itself, and holds these data in the memory as the setting data 43 and policy data 44.

[0023] FIG. 4 shows an example of information contents held as the setting data 31 and the setting data 43. As shown in FIG. 4, in this example, the encryption method when the computer equipment to be managed 4 (equipment to be managed R1) communicates with other computer equipment to be managed (equipment to be managed R2) is "DES" (Data Encryption Standard), the cryptographic key length is "56", the authentication method is "MD5", and the communication bandwidth is "7 Mbps" (7 megabits per second). Other than these setting information, specified values of the setting information that are required by the OS (Operating System) mounted on the computer equipment to be managed 4, or the network function are included in the setting data.

[0024] Moreover, FIG. 5 shows an example of the information contents held as the policy data 32 and the policy data 44. As shown in FIG. 5, each item name of the policy data corresponds to each setting information name of the setting data shown in FIG. 4. The countermeasure (corrective action) to be taken when incorrect

setting is detected by means of a check described later, is held for each setting information name.

[0025] In this example, corrective action is decided such that when disagreement is found between the specified value to be set and an actually set value, the specified value is set by means of overwrite, respectively, with regard to the encryption method used between equipment to be managed R1 and the equipment to be managed R2, the cryptographic key length used between equipment to be managed R1 and the equipment to be managed R2, and the authentication method used between equipment to be managed R1 and the equipment to be managed R2. Furthermore, corrective action is decided for the communication bandwidth such that when disagreement is found in the communication bandwidth used between equipment to be managed R1 and the equipment to be managed R2, this is notified by e-mail to a mail address "admin@nec.co.jp".

[0026] Next, a description is given of a procedure for monitoring the setting of the computer equipment to be managed 4 and executing the processing based on the policy, using the setting data 43 and the policy data 44 whose contents are held as shown in the figure, in accordance with the above described method. FIG. 3 is a flow chart showing a procedure for the monitoring processing by the policy application operation section 42.

[0027] The policy application operation section 42 receives a notification from the timer 45 when a predetermined time has passed after completion of the former processing. Therefore, the policy application operation section 42 first checks whether the predetermined time has already passed or not, in step S201 in FIG. 3. If the predetermined time has not passed yet, the policy application operation section 42 repeats the processing of step S201, while on the other hand, if the predetermined time has already passed, the policy application operation section 42 shifts the processing to the next step S202.

[0028] After the above-described predetermined time has passed, the policy application operation section 42 reads out the setting information 46 in step S202. Then, the policy application operation section 42 reads out the setting data 43 in step S203, and compares the set value in the setting information 46 with the specified value in the setting data 43, with regard to respective setting items.

[0029] As a result of the comparison, if disagreement is not found between these, the processing proceeds to step S205 to complete the processing. On the other hand, if any disagreement is found between these, the processing proceeds to step S204 to read the policy data 44. Then, according to the countermeasure written in the policy data 44, the countermeasure is executed with respect to the information item where disagreement has been found.

[0030] For example, it is assumed that the "crypto-

graphic key length with R2" defined in the setting information 46 is not "56" defined in the setting data 43 shown in FIG. 4, but is altered to "128" for some reason or other. In this case, the policy application operation section 42 reads out the information related to the "cryptographic key length with R2" defined in the policy data 44 shown in FIG. 5, and rewrites the "cryptographic key length with R2" set as the setting information 46 as "56", in accordance with "overwrite" being the predetermined countermeasure.

[0031] In this manner, if the corrective action is "overwrite", even if the setting information 46 has been altered due to carelessness or a malicious intention, the policy application operation section 42 resets it using the specified value. Hence the setting as per the intention of the administrator can be maintained.

[0032] For example, it is also assumed that the "communication bandwidth with R2" set in the setting information 46 is not "7 Mbps" defined in the setting data 43 shown in FIG. 4, but is altered to "5 Mbps" for some reason or other. In this case, the policy application operation section 42 reads out the information related to the "communication bandwidth with R2" defined in the policy data 44, and in accordance with "mailto:admin@nec.co.jp" being the predetermined countermeasure, sends mail for reporting that disagreement has been detected, to this address.

[0033] In the example shown in FIG. 5, one corrective action is defined for one information item, but a plurality of corrective actions may be taken. For example, both of correction of the setting value by means of "overwrite" and mail transmission by means of "mailto:" may be executed.

[0034] Then, after the above described series of processing have been completed in step S205, regardless of whether disagreement is found or not in step S203, the policy application operation section 42 again waits for the notification of passing of the predetermined time from the timer 46. As a result, it becomes possible to monitor the monitor setting information, not only at a certain point of time but also continuously, to thereby obtain an effect of improvement in security or the like.

[0035] Here, the above described policy management operation section 21 and policy application operation section 42 can be realized as a function of the computer program. This computer program is recorded on a recording medium used by the computer system, and the computer reads out and executes this program, to thereby perform the processing by the above described respective operation sections.

[0036] That is to say, the computer program recorded on the recording medium is loaded on a main memory (not shown) on the computer equipment to be managed 4, and a central processing unit (not shown) on the computer equipment to be managed 4 executes instructions described in the computer program one by one.

[0037] The process in which the computer reads

out the computer program involves read out via the communication network. The recording medium used by the computer system is a floppy disk, a magneto-optical disk, a CD-ROM (Compact Disc Read Only Memory), a magnetic hard disk, a semiconductor memory or the like, but the recording medium is not limited thereto.

[0038] As described above, according to this embodiment, specified values related to the setting information are held in the setting data 43 of the computer equipment to be managed 4, and these specified values are regularly compared with set values actually set in the setting information 46 of the computer equipment to be managed 4. Hence, even if the setting information on the computer equipment to be managed side has been altered due to carelessness of an administrator of the individual computer equipment to be managed, or a malicious intention of an attacker being a third party, to cause disagreement between the above described specified value and the set value, such an alteration of the setting information can be detected.

[0039] Moreover, when disagreement is detected, the policy in the countermeasure specified in advance and held in the computer equipment to be managed 4 as the policy data 44 is referred to, and the corresponding corrective action is automatically taken. Hence, it becomes possible to take appropriate action according to the specified corrective action, such as automatic restoration of the setting information, notification by means of automatic mail transmission to an administrator or the like. As a result, the setting information of the whole system can be maintained as per the intention of the administrator, thereby enabling prevention against an attack from an attacker.

[0040] Furthermore, the above described setting data 43, policy data 44 and setting information 46 are all held in the computer equipment to be managed 4, and processing performed by the policy application operation section 42 is also executed on the computer equipment to be managed 4. Hence the flow of these data on the network due to this processing, and the resultant imposition of a burden on the network resources can be avoided.

[0041] The setting data 31, 43 and the policy data 32, 44 are also uniformly managed by the policy management operation section 21, enabling input and editing on the operation terminal 1. Hence, it becomes possible to collectively manage the computer equipment connected to the network efficiently, enabling a decrease in management expenses.

[0042] In addition, the computer equipment to be managed 4 comprises the timer 45 for performing a timing function. For example, this timing function is associated with the timer program in the above described computer program, thereby enabling repetition of processing of the above described comparison check at regular intervals. As a result, alteration of the setting information can be monitored continuously.

[0043] This invention may be embodied in other forms or carried out in other ways without departing from the spirit thereof. The present embodiments are therefore to be considered in all respects illustrative and not limiting and all modifications falling within the meaning and range of equivalency are intended to be embraced therein.

Claims

1. A distributed remote management method for computer equipment for maintaining in appropriate condition setting information of computer equipment to be managed (4) connected to a network, comprising the steps of:

a first step for writing in advance specified values (43) of said setting information and countermeasures (44) when disagreement is found between a set value of said setting information and said specified value, in a memory provided in said computer equipment to be managed, based on the information managed by a management server (2) connected to said network; a second step in which a management unit provided in said computer equipment to be managed reads out said specified value from said memory;

a third step in which said management unit reads out a set value (46) actually set as said setting information;

a fourth step in which said management unit determines whether said specified value agrees with said set value or not;

a fifth step in which said management unit reads out said countermeasure from said memory, when disagreement is found in said fourth step; and

a sixth step for executing said countermeasure obtained in said fifth step.

2. A distributed remote management method for computer equipment according to claim 1, wherein a trigger is applied to said management unit by a timer (45) at regular intervals, and said management unit repeatedly executes said second to sixth steps based on this trigger.

3. A distributed remote management method for computer equipment according to claim 1 or 2, wherein

in said first step, a plurality of said countermeasures are written for each information item of said setting information;

in said fifth step, said plurality of countermeasures are read out from said memory; and

in said sixth step, said plurality of countermeasures are executed.

4. A distributed remote management method for computer equipment according to claim 1, 2 or 3, wherein in said sixth step, as said countermeasure, the set value of said setting information is overwritten with said specified value. 5
5. A distributed remote management method for computer equipment according to claim 1, wherein in said sixth step, as said countermeasure it is reported to a predetermined address to be notified that disagreement has been found. 10
6. A computer program product including a computer-readable control program recorded on a computer-usable medium, wherein 15
- said control program operates on computer equipment to be managed (4), for maintaining in an appropriate condition setting information of said computer equipment to be managed connected to a network, and executes: 20
- first processing for receiving and writing in advance to memory from a management server (2) connected to said network, specified values (43) of said setting information, and countermeasures (44) when disagreement is found between a set value of said setting information and said specified value, for carrying out against said disagreement; 25
- second processing for reading out said specified value from said memory; 30
- third processing for reading out a set value (46) actually set as said setting information; 35
- fourth processing for determining whether said specified value agrees with said set value or not; 40
- fifth processing for reading out said countermeasure from said memory, when disagreement is found in said fourth processing; and
- sixth processing for executing said countermeasure obtained in said fifth processing. 45
7. A computer program comprising program code for carrying out the method steps of any one of claims 1 to 5. 50
- 55

FIG. 1

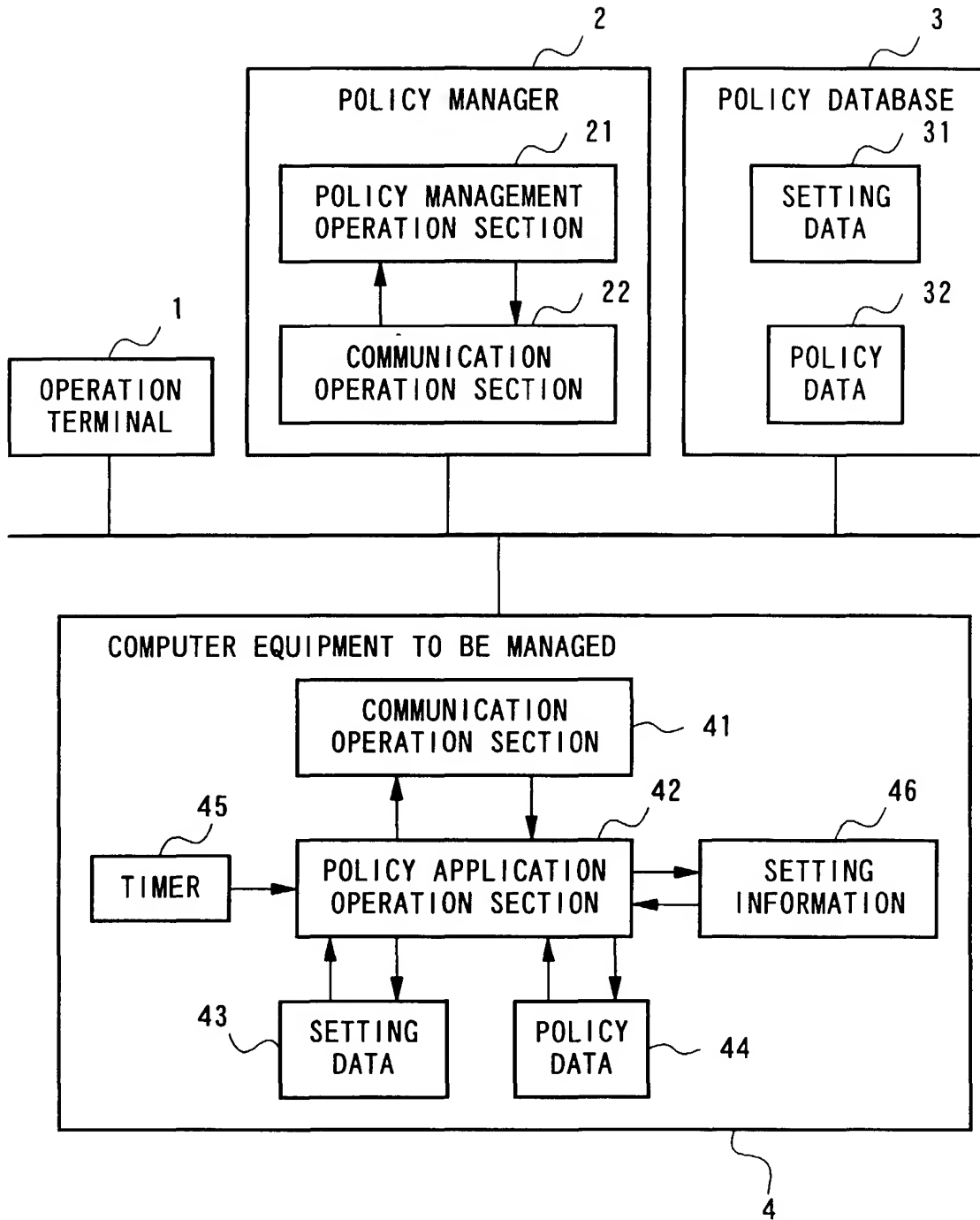


FIG. 2

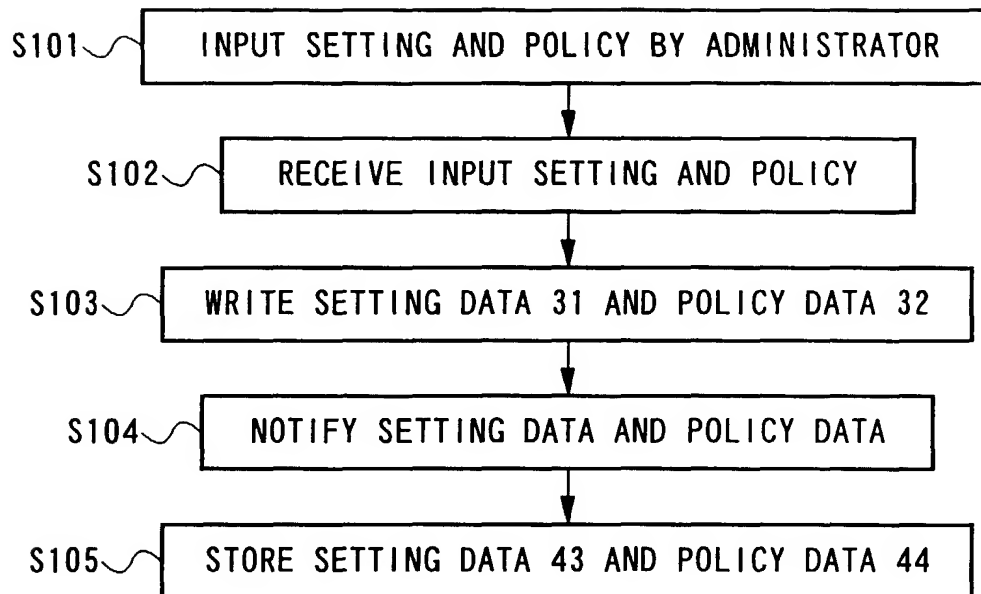


FIG. 3

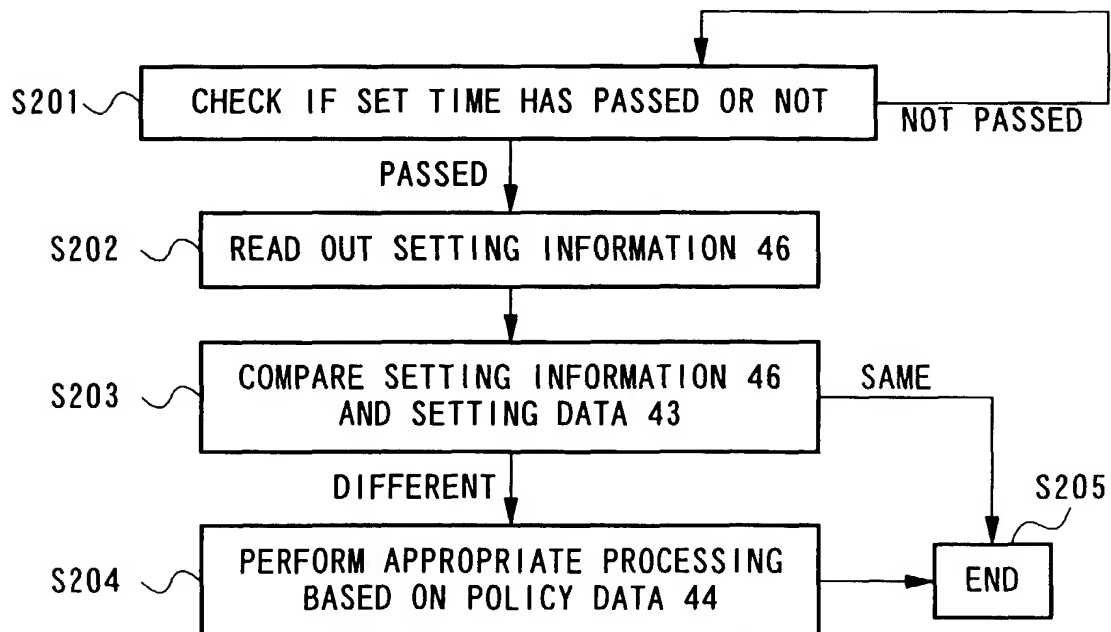


FIG. 4

EQUIPMENT NAME	IP ADDRESS	SETTING INFORMATION NAME	SET VALUE
EQUIPMENT TO BE MANAGED R1	111.5.9.5	ENCRYPTION METHOD WITH R2	"DES"
		CRYPTOGRAPHIC KEY LENGTH WITH R2	56
		AUTHENTICATION METHOD WITH R2	"MD5"
		COMMUNICATION BANDWIDTH WITH R2	7 Mbps
		:	
EQUIPMENT TO BE MANAGED R2	111.5.9.8	:	
:			

FIG. 5

EQUIPMENT NAME	ITEM NAME	COUNTERMEASURE
EQUIPMENT TO BE MANAGED R1	ENCRYPTION METHOD WITH R2	OVERWRITE
	CRYPTOGRAPHIC KEY LENGTH WITH R2	OVERWRITE
	AUTHENTICATION METHOD WITH R2	OVERWRITE
	COMMUNICATION BANDWIDTH WITH R2	mailto:admin@nec.co.jp
	:	
EQUIPMENT TO BE MANAGED R2 :		



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 00 12 0098

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	US 5 287 505 A (CALVERT NATHANIEL ET AL) 15 February 1994 (1994-02-15) * abstract; claims 1-13 *	1-7	G06F11/273 G06F11/22
A	US 5 155 847 A (PORRETT WILLIAM A ET AL) 13 October 1992 (1992-10-13) * abstract *	1-7	
			TECHNICAL FIELDS SEARCHED (Int.Cl.7)
			G06F
The present search report has been drawn up for all claims			
Place of search THE HAGUE		Date of completion of the search 31 January 2001	Examiner Sarasua, L.
<p>CATEGORY OF CITED DOCUMENTS</p> <p>X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document</p> <p>T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document</p>			

EPO FORM 1503 03/92 (P04C01)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 00 12 0098

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

31-01-2001

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5287505 A	15-02-1994	DE 68920462 D	23-02-1995
		DE 68920462 T	13-07-1995
		EP 0333620 A	20-09-1989
		JP 1243135 A	27-09-1989
		JP 1916596 C	23-03-1995
		JP 6044242 B	08-06-1994
US 5155847 A	13-10-1992	CA 1310131 A	10-11-1992